

INTERNAL AUDIT FOLLOW UP FORM

AUDIT	Payment Card Industry Standards	PREPARED BY	Lorraine Sarson	DATE	29 October 2010
REPORT DATED	29 July 2010	REVIEWED BY		PAGE	1 OF 6

NO	RECOMMENDATIONS	RESPONSIBLE OFFICER	DATE TO BE ACTIONED BY	CURRENT STATUS	MANAGEMENT RESPONSE	CURRENT COMMENTS
1	Risk: Identity and Financial Theft - Corporate Policies and Procedures					
1.1	The current Retention and Disposal policy should be updated to include the length of time credit/debit card receipts should be retained and how they should be disposed off for both chip and pin, and non chip and pin transactions. Priority: Medium	Data Protection Officer	August 2010		This will be updated as part of the re-continuation of the PCI compliance project. This area can be targeted for immediate update.	Being implemented
2	Risk: Identity and Financial Theft - Testing of sites with payment card facilities.					
2.1	All debit/credit card machines should be re-programmed to comply with the PCI guidance that only the first 6 and last 4 digits should be visible as a maximum. Priority: High	Group Finance Manager - Technical	August 2010		Agree	Implemented
2.2	All receipts should be held securely to prevent unauthorised access to confidential information. Priority: Medium	General Manager – Enterprise Works	August 2010		Agreed – will be taken up with the Enterprise Works Manager	Implemented - During the month all receipts are held securely in a locked safe and at month end after reconciliation they are transferred to a locked cabinet in our archive area.

Status: 1=Implemented, 2=Being Implemented, 3=Not Implemented, 4=Superseded, 5=Other

INTERNAL AUDIT FOLLOW UP FORM

AUDIT	Payment Card Industry Standards	PREPARED BY	Lorraine Sarson	DATE	29 October 2010
REPORT DATED	29 July 2010	REVIEWED BY		PAGE	2 OF 6

NO	RECOMMENDATIONS	RESPONSIBLE OFFICER	DATE TO BE ACTIONED BY	CURRENT STATUS	MANAGEMENT RESPONSE	CURRENT COMMENTS
2	Risk: Identity and Financial Theft - Testing of sites with payment card facilities.					
2.3	<p>Clarification should be provided by Corporate Finance to advise the correct length of time that credit/debit card receipts should be retained and then communicated to all departments.</p> <p>Records held that are over 7 years old should be disposed of securely.</p> <p>Priority: High</p>	<p>Group Finance Manager - Technical</p> <p>General Manager – STEAM</p>	<p>August 2010</p> <p>August 2010</p>		Agreed	Being implemented – policy being amended to 6 months retention as needed for chargebacks
2.4	Telephone Payment Request sheets should be disposed of promptly and securely once the transaction has been processed electronically.	Information Centre Manager	August 2010		<p>Response by J Leard, Visitor Information Centre Manager</p> <p>As soon as the transaction has been processed the Telephone Payment Request sheets are promptly held in the safe, which is only accessible by the responsible key holders. After a period of 6 months they are shredded by a cross-shredder. They are kept for a period of 6 months, as this is a requirement in case of charge-backs.</p>	Implemented and confirm all completed records are held in the safe and records older than 6 months are cross-shredded.

Status: 1=Implemented, 2=Being Implemented, 3=Not Implemented, 4=Superseded, 5=Other

INTERNAL AUDIT FOLLOW UP FORM

AUDIT	Payment Card Industry Standards	PREPARED BY	Lorraine Sarson	DATE	29 October 2010
REPORT DATED	29 July 2010	REVIEWED BY		PAGE	3 OF 6

NO	RECOMMENDATIONS	RESPONSIBLE OFFICER	DATE TO BE ACTIONED BY	CURRENT STATUS	MANAGEMENT RESPONSE	CURRENT COMMENTS
2	Risk: Identity and Financial Theft - Testing of sites with payment card facilities.					
2.5	Cardholder's security codes should not be kept once payment has been processed, as this is in breach of PCI requirements. Priority: High	Information Centre Manager	August 2010		Response by J Leard, Visitor Information Centre Manager We will promptly devise a system whereby the 3-digit card security number is not recorded on the Telephone Payment Request sheet and once the transaction is processed the security number will be destroyed.	Implemented
2.6	The Council should introduce an additional security check to mitigate the chances of fraudulent payments being made to the Council. Priority: High	Group Finance Manager - Technical	August 2010		'For cardholder present transactions 'chip and pin' machines are to be used. The security number is not required for these transactions. For transactions where the cardholder is not present, the introduction of the paye.net system later in 2010 will allow for security card numbers to be taken. The use of these will be considered during its implementation. The Axis system does not have a 'field' for security numbers.'	Being implemented December 2010

Status: 1=Implemented, 2=Being Implemented, 3=Not Implemented, 4=Superseded, 5=Other

INTERNAL AUDIT FOLLOW UP FORM

AUDIT	Payment Card Industry Standards	PREPARED BY	Lorraine Sarson	DATE	29 October 2010
REPORT DATED	29 July 2010	REVIEWED BY		PAGE	4 OF 6

NO	RECOMMENDATIONS	RESPONSIBLE OFFICER	DATE TO BE ACTIONED BY	CURRENT STATUS	MANAGEMENT RESPONSE	CURRENT COMMENTS
3	Risk: Identity and Financial Theft - Testing of departments taking payment information over the telephone.					
3.1	The 3-digit security code should not be retained once processing has been undertaken, this information should be removed from any forms being held within the departments. Priority: High	Head of Finance Admin (Capita)	August 2010		Agreed	Implemented - everything is securely stored via the cashier process. During the training, the need to not record the 3 digit number will be re-iterated
3.2	Any employee responsible for taking credit/debit card payments over the telephone should be aware of the Payment Card Industry standards and be advised on the issue of best practice. Priority: Medium	Group Finance Manager - Technical	August 2010		All employees identified as responsible for taking payments were identified and invited to attend general PCI training, which includes some of the sections highlighted at 3.2 Training will again be undertaken as part of the restart of the PCI project.	Being implemented as part of training

Status: 1=Implemented, 2=Being Implemented, 3=Not Implemented, 4=Superseded, 5=Other

INTERNAL AUDIT FOLLOW UP FORM

AUDIT	Payment Card Industry Standards	PREPARED BY	Lorraine Sarson	DATE	29 October 2010
REPORT DATED	29 July 2010	REVIEWED BY		PAGE	5 OF 6

NO	RECOMMENDATIONS	RESPONSIBLE OFFICER	DATE TO BE ACTIONED BY	CURRENT STATUS	MANAGEMENT RESPONSE	CURRENT COMMENTS
----	-----------------	---------------------	------------------------	----------------	---------------------	------------------

3	Risk: Identity and Financial Theft - Testing of departments taking payment information over the telephone.					
3.3	Procedures need to be introduced to ensure all departments are aware of their responsibilities and that the practice of receiving payment card information over the telephone is consistent across the Council. Priority: High	Group Finance Manager - Technical	August 2010		Response by F Pearce Responsibility for reconciliation of TIC cash / card takings is the responsibility of Capita Finance Admin therefore we have to have the merchant copies. I would question this recommendation as the storage of merchant copies in central finance admin is more secure than TIC and does not negatively impact procedures, policy or security. Introducing Paye.net will address this issue.	Being implemented as part of PCI training
4	Risk: Financial loss to the Authority					

Status: 1=Implemented, 2=Being Implemented, 3=Not Implemented, 4=Superseded, 5=Other

INTERNAL AUDIT FOLLOW UP FORM

AUDIT	Payment Card Industry Standards	PREPARED BY	Lorraine Sarson	DATE	29 October 2010
REPORT DATED	29 July 2010	REVIEWED BY		PAGE	6 OF 6

NO	RECOMMENDATIONS	RESPONSIBLE OFFICER	DATE TO BE ACTIONED BY	CURRENT STATUS	MANAGEMENT RESPONSE	CURRENT COMMENTS
4.1	A list of sites included should be held with the contract and kept up to date, new sites should be added when identified as requiring this service. Priority: Medium	Group Finance Manager - Technical	August 2010		Unclear what the purpose of this recommendation is and what advantages this would bring.	Implemented

Status: 1=Implemented, 2=Being Implemented, 3=Not Implemented, 4=Superseded, 5=Other